Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 8 | Aug 2017

ENHANCING BASE STATION SECURITY IN WIRELESS SENSOR NETWORKS

R. Jayanthi [1] | A. Mercy Gnana Rani [1]

[1] M. Phil Research Scholar, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

[2] Assistant Professor, Department of Information Technology, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

ABSTRACT

Wireless sensor networks that are deployed in applications such as battlefield monitoring and home sentry systems face acute security concerns, including eavesdropping, forgery of sensor data, denial of service attacks, and the physical compromise of sensor nodes. Sensor networks are often organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource-constrained sensor nodes. Prior work that has focused on securing the routing between sensor nodes has assumed that the base station is sufficiently powerful to defend itself against security threats. This paper considers strategies for securing the sensor network against a variety of threats that can lead to the failure of the base station, which represents a central point of failure. First, multipath routing to multiple destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks and/or compromise. Second, confusion of address and identification fields in packet headers via hashing functions is explored as a technique to help disguise the location of the base station from eavesdroppers. Third, relocation of the base station in the network topology is studied as a means of enhancing resiliency.

KEYWORDS: Security, Multihop, Eavesdropping.

I. INTRODUCTION:

Wireless sensor networks are rapidly growing in popularity. Applications of sensor networks that have emerged include habitat monitoring, robotic toys, and battlefield monitoring. A wide range of applications are emerging, including location aware sensor networks in the home and office, assistive technology for biomedical sensing, and outdoor deployments of sensor networks to monitor storms, oceans, and weather events. For military deployments, security is essential to protect the routing infrastructure and packet data from threats such as eavesdropping, tampering, denial-of-service (DOS) attacks, and the physical compromise of sensor nodes deployed into enemy territory.

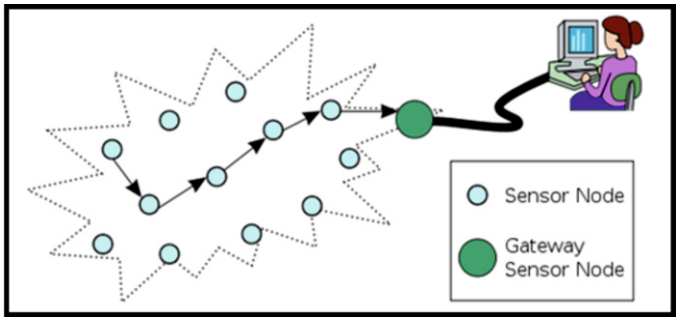

Figure 1.1 WSN architecture

The research challenge is to secure the routing infrastructure against such threats given the severe resource constraints imposed by wireless sensor networks. Wireless sensor networks consist of individual sensor nodes that are highly resource-constrained in terms of their limited energy lifetime, modest CPU, and scant memory. While it has been demonstrated that symmetric key cryptography can be implemented on today's wireless sensor platforms initial results indicate that public key cryptography remains out of reach for today's sensor networks due the compute-intensive nature of public key methods. Prior work in securing wireless sensor networks therefore focuses on exploiting symmetric key-based techniques for achieving authentication, data integrity, and confidentiality. As a result, a key focus of this paper concerns security obtained through symmetric key cryptography.

A notable feature of the architecture of a wireless sensor network is its hierarchy, rooted in a base station. The base station is typically resource-rich in terms of its computational ability, storage capacity, and energy lifetime compared to individual sensor nodes.

Providing location privacy in a sensor network is challenging. First, an adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. He can use information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. Second, sensors usually have limited processing speed and energy supplies. It is very expensive to apply traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks. We need to find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes.

III. ADVANTAGES OF WIRELESS SENSOR NETWORKS:

Recently, a number of privacy-preserving routing techniques have been developed for sensor networks. However, most of them are designed to protect against an adversary only capable of eavesdropping on a limited portion of the network at a time. A highly motivated adversary can easily eavesdrop on the entire network and defeat these schemes. For example, the adversary could deploy his own set of sensor nodes to monitor the communications in the target network. This is especially true in a military or industrial spying context, where the adversary has strong, potentially life-or-death, incentives to gain as much information as possible from observing the traffic in the target network. Given a global view of the network traffic, the adversary can easily infer the locations of monitored objects and sinks. For example, a region in the network with high activity should be close to a sink, while a region where the packets originate should be close to a monitored object. In this paper, we focus on privacy-preserving communication methods in the presence of a global eavesdropper who has a complete view of the network traffic.

The assumption of a global eavesdropper can monitor the entire network traffic, is often realistic for highly motivated adversaries. We then formalize the location privacy issues under such an assumption and apply an analysis based on Steiner trees to estimate the minimum communication cost required to achieve a given level of privacy. We provide the first formal study of how to quantitatively measure location privacy in sensor networks. We then apply the results of this study to evaluate our proposed techniques for location privacy in sensor networks. These include two techniques that hide t he locations of monitored objects—periodic collection and source simulation and two techniques that provide location privacy to data sinks—sink simulation and backbone flooding. Our analysis and simulation studies show that these approaches are effective and efficient.

VI. EXISTING APPROACHES:

Location privacy has been an active area of research in recent years. In location-based services, a user may want to retrieve location-based data without revealing her location. Techniques such as k-anonymity and private information retrieval have been developed for this purpose. In pervasive computing, users' location privacy can be compromised by observing the wireless signals from user devices. Random delay and dummy traffic have been suggested to mitigate these problems. Location privacy in sensor networks also falls under the general framework of location privacy. The adversary monitors the wireless transmissions to infer locations of critical infrastructure. However, there are some challenges unique to sensor networks. First, sensor nodes are usually battery powered, which limits their functional lifetime. Second, a sensor network is often significantly larger than the network in smart home or assisted living applications.

Source-location privacy:

Prior work in protecting the location of monitored objects sought to increase the safety period, i.e., the number of messages sent by the source before the object is

located by the attacker. The flooding technique has the source node send each packet through numerous paths to a sink, making it difficult for an adversary to trace the source. Fake packet generation creates fake sources whenever a sender notifies the sink that it has real data to send. The fake senders are away from the real source and approximately at the same distance from the sink as the real sender. Phantom single-path routing achieves location privacy by making every packet walk along a random path before being delivered to the sink. Cyclic entrapment creates looping paths at various places in the network to fool the adversary into following these loops repeatedly and thereby increase the safety period. However, all these techniques assume a local eavesdropper who is only capable of eavesdropping on a small region. A global eavesdropper can easily defeat these schemes by locating the first node initiating the communication with the base station.

Sink-location privacy:

In [6], Deng et al. described a technique to protect the locations of sinks from a local eavesdropper by hashing the ID field in the packet header. In [8], it was shown that an adversary can track sinks by carrying out time correlation and rate monitoring attacks. To mitigate these two kinds of attacks, Deng et al. introduced a multiple-parent routing scheme, a controlled random walk scheme, a random fake path scheme, and a hot spots scheme [8]. In [13], redundant hops and fake packets are added to provide privacy when data are sent to the sink. However, these techniques all assume that the adversary is a local eavesdropper. A global eavesdropper can easily defeat these schemes. For example, the global eavesdropper only needs to identify the region exhibiting a high number of transmissions to locate the sink. We, thus, focus on privacy preserving techniques designed to defend against a global eavesdropper.

V. PRIVACY-PRESERVING ROUTING:

In this section, the proposed privacy-preserving techniques for protecting the location information of monitored objects and data sinks are presented. It is assumed that all communications between sensor nodes in the network are encrypted using key predistribution protocols so that the contents of packets appear random to the global eavesdropper.

Source-Location Privacy Techniques:

Two techniques are presented to provide location privacy to monitored objects in sensor networks, periodic collection and source simulation. The periodic collection method achieves the optimal privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication overhead, and latency.

VI. CONCLUSION:

Prior work on location privacy assumes local eavesdropper in sensor networks. In case of highly motivated attacker it is unrealistic. This paper formalizes location privacy issues under a global eavesdropper. This paper presented techniques to provide location privacy to objects and sinks against a global eavesdropper.

.

REFERENCES:

1. A. Mainwaring, J. Polastre, R. Szewczyk D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring", First ACM Workshop on Wireless Sensor Networks and Applications (WSNA) 2002, pp. 88-97.
2. F. Martin, B. Mikhak, and B. Silverman, "MetaCricket: A designer's kit for making computational devices," IBM Systems Journal, vol. 39, nos. 3 & 4, 2000.
3. ARGUS Advanced Remote Ground Unattended Sensor Systems, Department of Defense, U.S. Air Force, http://www.globalsecurity.org/intell/systems/arguss.htm.
4. D. Ganesan, R. Govindan, S. Shenker and D. Estrin, "Highly Resilient, Energy Efficient Multipath Routing in Wireless Sensor Networks," Mobile Computing and Communication Review (MC2R) Vol 1., No.2. 2002.
5. A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001, July 2001.
6. Y. Hu, D. Johnson, A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02).
7. Y. Hu, A. Perrig, D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002).
8. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, "System architecture directions for network sensors", ASPLOS 2000.
9. J. Staddon, D. Balfanz, G. Durfee, "Efficient Tracing of Failed Nodes in Sensor Networks", First Workshop on Sensor Networks and Applications, WSNA'02, Atlanta, Georgia, USA.
10. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
11. A. Wood, J. A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, 35(10):54-62, October 2002.
12. J. Deng, R. Han and S. Mishra, "The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks", to appear in IEEE 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03), Palo Alto, CA, USA, April, 2003.
13. P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet, In ASPLOS 2002, 2002.
14. Y. Hu, A. Perrig, D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", Technical Report TR01-384, Department of Computer Science, Rice University, June 2002.
15. J. J. Kong, P. Zerfos, H. Luo, S. Lu, L.X. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks", International Conference on Network Protocols (ICNP 2001).